(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日:
2005年11月24日(24.11.2005)

PCT

(10) 国际公布号:
WO 2005/112338 A1

(51) 国际分类号[7]: H04L 9/32, 12/56, H04Q 7/38

(21) 国际申请号: PCT/CN2005/000133

(22) 国际申请日: 2005年1月31日(31.01.2005)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200410005740.0 2004年2月16日(16.02.2004) CN

(71) 申请人(对除美国以外的所有指定国): 华为技术有限公司(HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人;及

(75) 发明人/申请人(仅对美国): 严军(YAN, Jun) [CN/CN]; 吴东君(WU, Dongjun) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京集佳知识产权代理有限公司 (UNITALEN ATTORNEYS AT LAW); 中国北京市朝阳区建国门外大街22号赛特广场7层, Beijing 100004 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

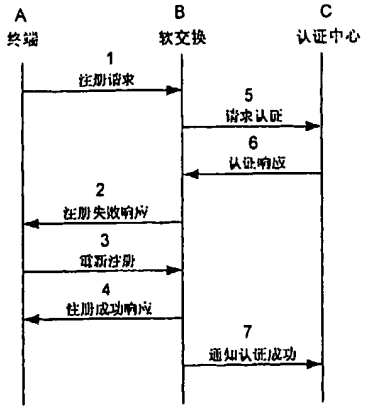
(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号, 请参考刊登在每期PCT公报期刊起始的"代码及缩写符号简要说明"。

(54) Title: KEY DISTRIBUTION METHOD

(54) 发明名称: 密钥分发方法



A TERMINAL
B SOFTSWITCH
C AUTHENTICATION CENTER
1 REGISTRATION REQUEST
2 REGISTRATION FAILURE RESPONSE
3 RE-REGISTER
4 REGISTRATION SUCCESS RESPONSE
5 AUTHENTICATION REQUEST
6 AUTHENTICATION RESPONSE
7 AUTHENTICATION SUCCESS NOTIFY

(57) Abstract: A key distribution method for the next generation network (NGN), includes: (a) a terminal sending a registration request message to a softswitch; (b) the softswitch sending a authentication request message to a authentication center; (c) the authentication center authenticating the terminal, then the softswitch distributing the session key to the terminal after the registration authentication being passed. The invention implements the key distribution during the registration authentication, thus the traffic is less, and it could combine the specialty of the NGN, and improve the efficiency for solving the security problem, the registration authentication of the terminal and the distribution of the key are more fit for the NGN actually.

WO 2005/112338 A1

[见续页]

(57) 摘要

本发明公开一种密钥分发方法，应用于下一代网络中，主要包括如下步骤：a）终端向软交换发送注册请求消息；b）软交换向认证中心发送认证请求消息；c）认证中心对终端进行认证，同时生成所述终端与软交换的会话密钥，并在注册认证通过后，交由软交换向终端分发所述会话密钥。本发明由于在注册认证过程中实现密钥的分发，通信量小，能紧密的结合 NGN 网络的特点、同时又大大提高了整个系统解决安全问题的效率，终端的注册认证与密钥的集中分发更适合于 NGN 网络的实际情况。

密钥分发方法

技术领域

本发明涉及通信中的安全管理技术，尤指一种应用于 NGN（下一代网络）中的密钥分发方法。

背景技术

NGN是可以提供包括话音、数据和多媒体等各种业务在内的综合开放的网络构架，为用户提供实时的会话业务。其网络设备包括少量的核心设备和大量的用户终端，网络中除了与PSTN/PLMN（公众电信网/公众陆地移动网）的交互是基于电路方式而比较安全外，其它网络设备之间的交互，都是基于分组核心网络及各种分组接入网络来传送。在开放的IP网络上，NGN网络极易受到各种非法的攻击，特别是NGN网络中存在的大量的分组终端，很容易成为非法攻击的发起者。

针对 NGN 网络安全，目前还没有较好的解决方案，而作为网络安全基础的密钥分发过程如何和 NGN 网络的特点结合起来，还是一个空白。现有技术中网络层安全标准 IPSec（网络层安全）定义的密钥协商方式是 IKE 协议（因特网密钥交换协议）、传输层安全标准 TLS（传输层安全）的密钥协商方式，由 TLS 规范定义的 Handshake（握手协议）来完成，其中 IKE 协议的密钥加密交换采用 Diffie-Hellman 算法，该算法定义了 5 个 D-H 算法的参数组（即素数 p 和底数 g），该加密算法具有强度高、密钥长度大的特点。从上可知，IKE 是一个非常严谨、同时也是一个相当复杂的密钥交换协议，而 Handshake 协议实现客户和服务器之间的一方（主要对服务器）或双向认证，协商协议中用到的加密算法和密钥以及验证算法和密钥，协商得到的会话参数供记录协议为多个连接重复使用，避免每个连接协商新的会话参数所带来的开销，同时协议保证协商过程是可靠的、协商得到的共享密钥是安全的。

尽管上述这些密钥分发协议都很规范、严谨，但都存在无法和

NGN 网络的实际特点相结合的缺点。NGN 网络是一个较为封闭的网络，由一系列网络侧服务器（如软交换、应用服务器和各种网关）以及大量的接入终端组成，终端和网络设备在一个运营商的管辖和控制范围内，存在一个管理域对域内设备进行管理，以及协助完成跨域之间用户互通的特点，同时所有的终端需要在该管理域内进行注册，NGN 的这些网络特点决定了 NGN 适合于采用集中式的密钥分发方式，而上述密钥分发协议都是终端之间或两台主机直接进行密钥的协商，最终导致系统中的通信量呈几何数的增长，使系统密钥分发效率较低，给整个网络系统和密钥的管理都带来了很大的不便，不适应 NGN 网络的实际特点。

发明内容

本发明解决的技术问题是提供一种安全、高效的密钥分发方法，可实现集中密钥分发，适应 NGN 的网络特点、使用方式灵活。

为解决上述问题，本发明提供一种密钥分发方法，应用于包括终端、软交换及认证中心的下一代网络中，该方法包括如下步骤：

a）终端向软交换发送注册请求消息请求注册；

b）软交换向认证中心发送认证请求消息请求对终端的认证；

c）认证中心对终端进行认证，同时生成所述终端与软交换的会话密钥，并在注册认证通过后，交由软交换向终端分发所述会话密钥。

其中，步骤 c）中，认证中心采用下述步骤对终端进行认证：

c1）认证中心根据与终端的共享密钥 Kc 生成对终端的第一验证字，然后以所述共享密钥 Kc 对所述会话密钥加密，将加密后的会话密钥和第一验证字返回给软交换；

c2）软交换向终端返回注册失败响应消息通知终端注册失败；

c3）终端根据与认证中心的共享密钥 Kc 生成第二验证字，然后向软交换发送包含所述第二验证字的注册消息重新进行注册；

c4）软交换根据所述第一验证字和所述第二验证字对所述终端进行认证。

其中，步骤 c）中，所述软交换采用下述步骤向终端分发所述会话密钥：

c5）软交换向终端返回注册成功响应消息，所述注册成功响应消息中包含经共享密钥 Kc 加密后的会话密钥，同时软交换向认证中心发出终端认证成功消息；

c6）终端根据所述共享密钥 Kc 解密认证中心加密过的会话密钥。

另外，所述方法还包括：所述终端向软交换发送本终端支持的安全能力列表及每种安全能力的优先级信息；

所述软交换根据所述终端的安全能力列表及每种安全能力的优先级信息选择一个合适的安全能力进行通信。

可选的，所述注册请求消息和注册消息均为 SIP 协议注册消息，所述注册失败响应消息为 SIP 协议响应消息，所述注册成功响应消息为 SIP 协议注册请求成功消息。

可选的，所述注册请求消息为 MGCP 协议系统重启消息及其响应消息，所述注册失败响应消息和注册成功响应消息均为 MGCP 协议通知请求消息及其响应消息，所述注册消息为 MGCP 协议通知消息及其响应消息。

可选的，所述注册请求消息为 H.248 协议系统服务状态变化消息及其响应消息，所述注册失败响应消息和注册成功响应消息均为 H.248 协议属性更改消息及其响应消息，所述注册消息为 H.248 协议通知消息及其响应消息。

可选的，所述注册请求消息为 H.323 协议网守请求消息，所述注册失败响应消息为 H.323 协议网守拒绝消息，所述注册消息为 H.323 协议注册请求消息，所述注册成功响应消息为 H.323 协议注册成功消息。

本发明还公开了另一种密钥分发方法，应用于包括终端、信令代理、软交换及认证中心的下一代网络中，该方法具体包括如下步骤：

A）终端通过信令代理向软交换发送注册请求消息请求注册；

B）软交换向认证中心发送认证请求消息请求对终端的认证；

C）认证中心对终端进行认证，同时生成所述终端与所述信令代理的会话密钥，并在注册认证通过后，交由软交换通过信令代理向终端分发所述会话密钥。

其中，步骤C）中，认证中心采用下述步骤对终端进行认证:

C1）认证中心根据与终端的共享密钥Kc以及与信令代理的共享密钥Ksp生成对终端的第一验证字，然后以所述共享密钥Kc和所述共享密钥Ksp分别对会话密钥进行加密，将加密后的会话密钥和所述第一验证字返回给软交换;

C2）软交换通过信令代理向终端返回注册失败响应消息通知终端注册失败;

C3）终端根据与认证中心的共享密钥Kc生成第二验证字，然后将包含所述第二验证字的注册消息发送给信令代理，由所述信令代理向软交换转发所述注册消息重新进行注册;

C4）软交换根据所述第一验证字和所述第二验证字对所述终端进行认证。

其中，步骤C）中，所述软交换采用下述步骤向终端分发所述会话密钥:

C5）软交换向信令代理转发终端注册成功响应消息，所述注册成功响应消息中包含认证中心分别以共享密钥Kc和Ksp加密后的会话密钥，信令代理用共享密钥Ksp解密认证中心经共享密钥Ksp加密过的会话密钥，并以所述解密获取的会话密钥对注册成功响应消息报文计算报文验证字，然后信令代理向终端转发注册成功响应消息，所述注册成功响应消息中包含经共享密钥Kc加密过的会话密钥以及所述报文验证字;

C6）终端根据所述共享密钥Kc解密认证中心加密过的会话密钥，并利用解密后获取的会话密钥，验证信令代理返回报文的报文验证字以验证信令代理身份，同时验证报文的完整性以及信令代理返回的终端自己的安全能力参数是否正确。

其中，终端将包含自身支持的安全能力列表以及每种安全能力的

优先级信息的注册消息发送给信令代理，信令代理根据终端支持的安全能力和每种安全能力的优先级信息选择一个合适的安全能力进行通信。

可选的，所述注册请求消息和注册消息均为 SIP 协议注册消息，所述注册失败响应消息为 SIP 协议响应消息，所述注册成功响应消息为 SIP 协议注册请求成功消息。

可选的，所述注册请求消息为 MGCP 协议系统重启消息及其响应消息，所述注册失败响应消息和注册成功响应消息均为 MGCP 协议通知请求消息及其响应消息，所述注册消息为 MGCP 协议通知消息及其响应消息。

可选的，所述注册请求消息为 H.248 协议系统服务状态变化消息及其响应消息，所述注册失败响应消息和注册成功响应消息均为 H.248 协议属性更改消息及其响应消息，所述注册消息为 H.248 协议通知消息及其响应消息。

可选的，所述注册请求消息为 H.323 协议网守请求消息，所述注册失败响应消息为 H.323 协议网守拒绝消息，所述注册消息为 H.323 协议注册请求消息，所述注册成功响应消息为 H.323 协议注册成功消息。

与现有技术相比，本发明具有以下优点：

1、本发明中由软交换与终端通信，在注册认证过程中实现密钥的分发，通信量小，能紧密的结合NGN网络的特点、同时又大大提高了整个系统解决安全问题的效率，终端的注册认证与密钥的集中分发更适合于NGN网络的实际情况。

2、本发明中可实现将SIP、MGCP、H.248、H.323等多个协议注册过程与会话密钥分发过程结合起来，在终端认证过程中完成会话密钥分发，后续的通信不需要再协商密钥，从而保证了密钥分发效率。

3、本发明中还可实现将 SIP、MGCP、H.248、H.323 等多个协议注册过程与安全能力协商过程结合起来，在密钥分发的过程中同时

完成安全能力协商，后续的通信不需要再协商安全能力，安全能力不需要进行静态配置，可动态协商，灵活扩展，因此使用方式灵活。

附图说明

图 1 是本发明密钥分发方法应用的一种 NGN 网络环境示意图；

图 2 是在图 1 所示的网络环境下本发明密钥分发方法具体实施例通信过程示意图；

图 3 是本发明密钥分发方法应用的具有信令代理的一种 NGN 网络环境示意图；

图 4 是在图 3 所示的网络环境下本发明密钥分发方法具体实施例通信过程示意图；

图 5 是在 SIP 协议注册认证过程中实现密钥分发的实施例通信过程示意图；

图 6 是在 MGCP 协议注册认证过程中实现密钥分发的实施例通信过程示意图；

图 7 是在 H.248 协议注册认证过程中实现密钥分发的实施例通信过程示意图；

图 8 是在 H.323 协议注册认证过程中实现密钥分发的实施例通信过程示意图。

具体实施方式

在 NGN 网络中，网络安全是目前 NGN 网络实际运营中碰到的一个重要问题，如果不能很好的解决 NGN 网络的安全问题，NGN 网络将无法得到大规模的应用。

在 NGN 网络中，网络设备主要包括终端、网关及软交换等，图 1 是 NGN 一种简单的单域组网图，即只有一个软交换（也称为媒体网关控制器）设备，实际组网可能有多个软交换设备。如图 1 所示的 NGN 网络环境中，软交换通过 IP 网络分别与中继媒体网关、SIP（会

话初始协议）终端，H.323 终端和 H.248 终端相连，其中中继媒体网关接模拟电话 T1、T2，另外软交换还与认证中心 AuC 相连。

本发明中所有网络设备、终端和认证中心 AuC 之间各有一个共享密钥，网络设备可以采用手工配置或网管下发，终端设备在设备开户时由系统分配或用户输入；

所有与认证中心 AuC 共享密钥为整个系统的基本密钥，需要得到妥善的保管，要求网络设备及终端具有不向第三方泄漏此密钥，以及具有抗非法盗取此密钥的能力；

另外，终端和软交换之间的会话密钥则由认证中心 AuC 生成。

本发明结合 NGN 网络的特点，通过将注册认证过程与会话密钥分发过程结合起来，在终端向软交换发起注册，软交换向认证中心请求认证后，认证中心生成终端与软交换的会话密钥，并在注册认证通过后，由软交换向终端分发会话密钥。由于在注册认证过程中完成会话密钥分发，后续的通信不需要再协商密钥，可使终端的注册认证和密钥的分发过程更简捷，提高了系统的效率和性能，对终端的要求较低，终端不需要支持复杂的密钥分发协议，而只需在现有的呼叫协议上扩展即可。

图 2 是一种简单的密钥分发通信过程示意图，说明如下：

终端首先向软交换发起注册请求，具体消息报文与终端支持的协议相关，软交换收到所述注册请求消息后，向认证中心请求对终端进行认证，认证中心根据终端信息生成相应验证字（便于区别以后称为第一验证字）以及会话密钥，然后向软交换返回认证响应消息，所述认证响应消息中包含所述第一验证字及会话密钥，软交换在收到所述认证响应消息后，向终端发送注册失败响应消息，要求终端重新注册，终端生成验证字（便于区别以后称为第二验证字），然后向软交换重新发起注册请求，软交换比较认证中心与终端提交的第一验证字和第二验证字，若不相同，则向终端返回注册失败响应消息，要求终端重新注册，若相同，则认证通过，向终端发送注册成功响应消息，所述

注册成功响应消息中包含会话密钥，终端在收到所述消息后即可获取会话密钥。

为了进一步提高网络的安全性，在软交换向终端返回注册失败响应消息时，软交换还要求终端反馈支持的安全能力列表，这样，终端重新向软交换发起注册时，在注册消息报文中进一步包括终端支持的安全能力列表以及每种安全能力的优先级信息等，软交换可据此选择合适的安全能力进行通信。

事实上为了通信的安全，本发明应用的网络环境中还可包括信令代理（SP），整个网络环境中，信令代理以上的网络设备之间的通信是可信的，即需要在组网上保证这些网络设备是处于一个信任区内，终端是不可信的，终端和信令代理之间的通信是不安全的，即终端和信令代理位于非信任区，信令代理为信任区和非信任区的边界。

本发明中信令代理可以是网络设备：宽带接入网关或边界会话控制器（SBC，Session Border Controller），具体实现时，可以作为一个功能模块与处理媒体转发的模块一起集成在 IP 网关中，也可以采用信令与媒体分离的架构方式，独立出来成为一个单独的信令代理实体，下面以具体实施例进行说明。

图 3 是一种信令代理集成在 IP 网关的网络环境，在所述的网络环境中，终端通过信令代理实现与软交换通信，上述终端与软交换的会话密钥在所述的网络环境中也即终端与信令代理的会话密钥。

图 4 是图 3 所示具信令代理的网络环境中实现密钥分发的通信过程，说明如下：

在步骤 s1.终端按协议流程向信令代理发送注册请求消息，正常的协议注册消息，具体消息报文与终端支持的协议相关，为一个普通的协议注册报文，报文未经加密认证处理，所述注册请求消息报文中包含如下信息：

IDc || IDsp || N1||TS1

– IDc：标识终端

– IDsp: 标识信令代理

– N1: 随机数或序列号，用于标识本次报文，返回的响应报文中需包含此数，用于防止报文重发（后续消息中的此数含义相同）

– TS1: 用于信令代理验证终端的时钟与信令代理的时钟是否同步;

在步骤 s2.信令代理向软交换转发终端的注册请求消息，该消息报文中包含如下信息:

IDc || IDsp

– IDc: 标识终端

– IDsp: 标识信令代理;

在步骤 s3.软交换没有终端的鉴权信息，向认证中心（AuC）发出对终端的鉴权认证请求消息，提供终端标识 ID 和信令代理标识 ID，该消息报文中包含信息如下:

IDc || IDsp

– IDc: 标识终端;

– IDsp: 标识终端接入网络的信令代理;

在步骤 s4.认证中心根据终端标识 ID、信令代理标识 ID，获取与终端的共享密钥 Kc 以及与信令代理的共享密钥 Ksp 及其它认证信息，生成一个挑战字随机数 Rand，由 Rand，IDc 和共享密钥 Kc 等一起生成对终端的第一验证字 Authenticatorc，同时生成终端和信令代理之间的会话密钥 Kc,sp，并分别由共享密钥 Kc 和 Ksp 对所述会话密钥 Kc,sp 加密，将 Rand、验证字、加密后的会话密钥 Kc,sp 作为软交换认证请求的响应返回给软交换，该认证响应消息报文中包含如下信息:

IDc || IDsp || Rand || Authenticatorc || EKc [Kc,sp] || EKsp [Kc,sp]

其中： Authenticatorc = f m(Kc， Rand， IDc)

– IDc: 标识终端

– IDsp : 标识信令代理

– Rand: 随机数，用于认证中心计算验证字，认证中心将 Rand 发给软交换，软交换再发给信令代理，再由信令代理发给终端

– Authenticatorc: 验证字，用于软交换验证终端，认证中心生成后发给软交换

– EKc [Kc,sp]: 认证中心以共享密钥 Kc 加密过的会话密钥 Kc,sp

– EKsp [Kc,sp]: 认证中心以共享密钥 Ksp 加密过的会话密钥 Kc,sp

在步骤 5.软交换向信令代理返回注册失败响应消息，注册失败，需要对终端进行认证，注册失败响应消息报文参数中包括挑战字 Rand，该消息报文中包含如下信息:

IDc || IDsp || Rand

– IDc: 标识终端

– IDsp: 标识信令代理

– Rand: 为认证中心发给信令代理的随机数;

在步骤 6.信令代理向终端返回注册失败响应消息，注册失败，需要对终端进行认证，同样注册失败响应消息报文中包括挑战字 Rand，同时要求终端反馈支持的安全能力列表和每种安全能力的优先级信息，该报文中包含如下信息:

IDc || IDsp || N1 || N2 || TS2 || Rand

– IDc: 标识终端

– IDsp: 标识信令代理

– N1: 同终端发给信令代理的注册消息报文中的 N1，用于对注册报文的回应

– N2: 用于标识本次报文

– TS2: 用于终端验证时间戳

– Rand: 为认证中心生成的随机数;

在步骤 7.终端通过共享密钥 Kc、客户段标识 IDc 及信令代理返

回的随机数 Rand 重新计算验证字，向信令代理重新发起注册，注册消息报文中包括新计算得到的第二验证字 Authenticatorc，同时注册消息报文中包含终端支持的安全能力列表（如网络层安全 IPSec、传输层安全 TLS 或应用层安全等），以及每一种安全能力的优先级信息，信令代理将根据终端的安全能力和优先级信息选择一个合适的安全能力进行通信，该注册消息报文中包含如下信息：

IDc || N1|| N2 || TS3 || Authenticatorc|| Security mechanism list

其中： Authenticatorc = f (Kc， Rand， IDc)

– IDc: 标识终端;

– N1: 新的随机数或序列号，用于标识本次报文

– N2: 用于标识对信令代理上一个报文的回应

– TS3: 让信令代理验证时间戳

– Authenticatorc: 验证字，由终端生成

– Security mechanism list: 终端的安全能力及优先级列表;

在步骤 8.信令代理向软交换转发终端的注册消息报文，对于终端的安全能力和优先级信息参数可以转发，也可以不转发，软交换不需该信息，该注册消息报文中包含如下信息：

IDc || IDsp||Authenticatorc

– IDc: 标识终端

– IDsp: 标识信令代理

– Authenticatorc: 验证字，由终端生成;

在步骤 9.软交换将信令代理发过来的注册消息报文中的第二验证字和认证中心发过来的第一验证字进行比较，对终端进行验证，若两者不一致，则验证失败，可重发注册失败响应消息，若两者一致，则表明对终端的验证成功，向信令代理返回注册成功响应消息报文，该消息报文中同时包括两个由认证中心生成的分别经过 Kc 和 Ksp 加密后的终端与信令代理之间的会话密钥 Kc,sp，该消息报文中包含如下信息：

IDc || IDsp || EKc[Kc,sp] || EKsp[Kc,sp]

– IDc: 标识终端

– IDsp: 标识信令代理

– EKc[Kc,sp]: 为认证中心用共享密钥 Kc 加密的终端与信令代理之间的会话密钥 Kc,sp

– EKsp[Kc,sp]: 为认证中心用共享密钥 Ksp 加密的终端与信令代理之间的会话密钥 Kc,sp;

在步骤 10.信令代理收到软交换的注册响应成功消息，向终端转发注册成功响应消息，该消息报文中包含由认证中心生成的经过终端的共享密钥 Kc 加密后的会话密钥 Kc,sp，同时注册成功响应消息中包括信令代理依据终端的安全能力参数选定的后续通信采用的安全能力项以及终端的安全能力参数列表和优先级信息（用于终端确认这些参数是否在网络传输中被第三者修改），最后用共享密钥 Ksp 对由认证中心生成的经过 Ksp 加密后的会话密钥 Kc,sp 进行解密处理，得到 Kc,sp，并用 Kc,sp 对整个响应消息报文计算报文验证字 MAC，用于保证报文的完整性，以及终端对信令代理的认证，报文中包含如下信息:

IDc || IDsp || N1 || N2 || TS4 || EKc[Kc,sp] || || Security mechanism || Security mechanism list(c) || fm（Kc,sp，报文）

– IDc: 标识终端

– IDsp: 标识信令代理

– N1: 用于标识对终端注册报文的回应

– N2: 用于标识本次报文

– TS4: 用于终端验证时间戳

– EKc[Kc,sp]: 为认证中心用共享密钥 Kc 加密的终端与信令代理之间的会话密钥 Kc,sp

– Security mechanism: 信令代理根据终端的安全能力及优先级列表选定的安全能力

– Security mechanism list: 终端自己的安全能力及优先级列表，用于终端确认信令代理收到的安全能力列表没有被非法修

改过

– fm（Kc,sp，报文）：用会话密钥 Kc,sp 对整个报文进行源和完整性认证，终端通过解开会话密钥，并对报文进行成功鉴别来实现对信令代理的身份认证，否则信令代理无法得到由认证中心签发的会话密钥 Kc,sp；

在步骤 11.软交换向认证中心发出终端认证成功消息，更新终端的相关信息，同时终端对由认证中心生成的经过 Ksp 加密后的会话密钥解密得到 Kc,sp，并用 Kc,sp 验证信令代理返回报文的 MAC，实现对信令代理的身份验证，同时验证报文的完整性，以及信令代理返回的终端自身的安全能力参数是否正确，如果正确，则说明信令代理返回的选定的安全能力正确，后续通信将按此安全能力进行报文安全处理，如果终端对信令代理认证失败或安全能力参数不正确，可重新发起注册，该终端认证成功消息报文中包含如下信息：

IDc || IDsp || IPc || …

– IDc：标识终端

– IDsp：标识信令代理

IPc：终端注册的 IP 地址，可能是经过信令代理变换处理后的 IP 地址。

下面以具体的应用协议环境对本发明密钥分发方法进行说明。

图 5 是本发明采用 SIP 协议进行注册认证的具体通信过程，仍以网络环境为具有信令代理为例，所述通信过程中只是将上述通用流程中的注册和响应消息细化为具体的 SIP 协议消息，流程中每一步骤的消息所携带的参数与上述通用流程中的定义是一致的。

所述通信过程中具体的协议消息，在步骤 s1、步骤 s2，注册请求消息为 SIP 协议中的注册消息；在步骤 s5、步骤 s6，注册失败响应消息为 SIP 协议中的响应消息代码，其中 401：为 SIP 协议中的响应消息代码，含义为需要对终端进行认证，407：为 SIP 协议中的响应消息代码，含义为需要对代理进行认证，在步骤 s7、步骤 s8，重新注册消息也为 SIP 协议中的注册消息；在步骤 s9、步骤 s10，注册

成功响应消息为 SIP 协议中的响应消息代码，表示请求成功，即 OK；而步骤 s3、s4、s11 中的消息，则与具体的呼叫协议没有关系，可以是通用的认证协议，根据应用场合的不同，可以采取不同的协议，如 Radius、Diameter 等。

图 6 是本发明采用 MGCP（媒体网关控制协议）协议进行注册认证的具体通信过程，仍以网络环境为具有信令代理为例，所述通信过程中只是将上述通用流程中的注册和响应消息细化为具体的 MGCP 协议消息，流程中每一步骤的消息所携带的参数与上述通用流程中的定义是一致的。

所述通信过程中具体的协议消息，在步骤 s1、步骤 s2，注册请求消息为 MGCP 协议中的系统重起消息命令 RSIP 及其响应消息；在步骤 s5、步骤 s6，注册失败响应消息为 MGCP 协议中的通知请求消息命令 RQNT，表示系统需要对终端进行认证，在步骤 s7、步骤 s8，重新注册消息为 MGCP 协议中的通知消息命令 NOTIFY，表示终端发起认证；在步骤 s9、步骤 s10，注册成功响应消息为 MGCP 协议中的通知请求消息命令 RQNT，通知终端认证成功；而步骤 s3、s4、s11 中的消息，则与具体的呼叫协议没有关系，可以是通用的认证协议，根据应用场合的不同，可以采取不同的协议，如 Radius、Diameter 等。

图 7 是本发明采用 H.248 协议进行注册认证的具体通信过程，仍以网络环境为具有信令代理为例，所述通信过程中只是将上述通用流程中的注册和响应消息细化为具体的 H.248 协议消息，流程中每一步骤的消息所携带的参数与上述通用流程中的定义是一致的。

所述通信过程中具体的协议消息，在步骤 s1、步骤 s2，注册请求消息为 H.248 协议中的系统服务状态变化消息命令 SERVICE CHANGE 及其响应消息 Rsp，此时表明系统开始进入服务状态，发起注册；在步骤 s5、步骤 s6，注册失败响应消息为 H.248 协议中的属性更改消息命令 MODIFY，表示系统需要对终端进行认证，在步骤 s7、步骤 s8，重新注册消息为 H.248 协议中的通知消息命令

NOTIFY，表示终端发起认证；在步骤 s9、步骤 s10，注册成功响应消息为 H.248 协议中的属性更改消息命令 MODIFY，通知终端认证成功；而步骤 s3、s4、s11 中的消息，则与具体的呼叫协议没有关系，可以是通用的认证协议，根据应用场合的不同，可以采取不同的协议，如 Radius、Diameter 等。

图 8 是本发明采用 H.323 协议进行注册认证的具体通信过程，仍以网络环境为具有信令代理为例，所述通信过程中只是将上述通用流程中的注册和响应消息细化为具体的 H.323 协议消息，流程中每一步骤的消息所携带的参数与上述通用流程中的定义是一致的。

所述通信过程中具体的协议消息，在步骤 s1、步骤 s2，注册请求消息为 H.323 协议中的 GK 请求消息，含义为谁是我的 GK；在步骤 s5、步骤 s6，注册失败响应消息为 H.323 协议中的 GK 拒绝消息，含义为 GK 不对终端进行注册，此处表示需要认证，在步骤 s7、步骤 s8，重新注册消息为 H.323 协议中的注册请求消息，此时消息中将携带认证信息，表示终端发起认证；在步骤 s9、步骤 s10，注册成功响应消息为 H.323 协议中的注册成功消息，通知终端认证成功；而步骤 s3、s4、s11 中的消息，则与具体的呼叫协议没有关系，可以是通用的认证协议，根据应用场合的不同，可以采取不同的协议，如 Radius、Diameter 等。

以上所述，仅为本发明的优选实施例而已，非因此即局限本发明的权利范围，凡运用本发明说明书及附图内容所为的等效变化，均理同包含于本发明的权利要求范围内。

权 利 要 求

1、一种密钥分发方法，应用于下一代网络中，所述下一代网络包括终端、软交换及认证中心，其特征在于，包括如下步骤:

a）终端向软交换发送注册请求消息请求注册;

b）软交换向认证中心发送认证请求消息请求对终端的认证;

c）认证中心对终端进行认证，同时生成所述终端与软交换的会话密钥，并在注册认证通过后，交由软交换向终端分发所述会话密钥。

2、根据权利要求 1 所述密钥分发方法，其特征在于，步骤 c）中，认证中心采用下述步骤对终端进行认证:

c1）认证中心根据与终端的共享密钥 Kc 生成对终端的第一验证字，然后以所述共享密钥 Kc 对所述会话密钥加密，将加密后的会话密钥和第一验证字返回给软交换;

c2）软交换向终端返回注册失败响应消息通知终端注册失败;

c3）终端根据与认证中心的共享密钥 Kc 生成第二验证字，然后向软交换发送包含所述第二验证字的注册消息重新进行注册;

c4）软交换根据所述第一验证字和所述第二验证字对所述终端进行认证。

3、根据权利要求 2 所述密钥分发方法，其特征在于，步骤 c）中，所述软交换采用下述步骤向终端分发所述会话密钥:

c5）软交换向终端返回注册成功响应消息，所述注册成功响应消息中包含经共享密钥 Kc 加密后的会话密钥，同时软交换向认证中心发出终端认证成功消息;

c6）终端根据所述共享密钥 Kc 解密认证中心加密过的会话密钥。

4、根据权利要求 3 所述密钥分发方法，其特征在于，所述方法还包括: 所述终端向软交换发送本终端支持的安全能力列表及每种安全能力的优先级信息;

所述软交换根据所述终端的安全能力列表及每种安全能力的优先级信息选择一个合适的安全能力进行通信。

5、根据权利要求 1-4 任一项所述密钥分发方法，其特征在于，所述注册请求消息和注册消息均为 SIP 协议注册消息，所述注册失败响应消息为 SIP 协议响应消息，所述注册成功响应消息为 SIP 协议注册请求成功消息。

6、根据权利要求 1-4 任一项所述密钥分发方法，其特征在于，所述注册请求消息为 MGCP 协议系统重启消息及其响应消息，所述注册失败响应消息和注册成功响应消息均为 MGCP 协议通知请求消息及其响应消息，所述注册消息为 MGCP 协议通知消息及其响应消息。

7、根据权利要求 1-4 任一项所述密钥分发方法，其特征在于，所述注册请求消息为 H.248 协议系统服务状态变化消息及其响应消息，所述注册失败响应消息和注册成功响应消息均为 H.248 协议属性更改消息及其响应消息，所述注册消息为 H.248 协议通知消息及其响应消息。

8、根据权利要求 1-4 任一项所述密钥分发方法，其特征在于，所述注册请求消息为 H.323 协议网守请求消息，所述注册失败响应消息为 H.323 协议网守拒绝消息，所述注册消息为 H.323 协议注册请求消息，所述注册成功响应消息为 H.323 协议注册成功消息。

9、一种密钥分发方法，应用于下一代网络中，所述下一代网络包括终端、信令代理、软交换及认证中心，其特征在于，包括如下步骤:

A）终端通过信令代理向软交换发送注册请求消息请求注册;

B）软交换向认证中心发送认证请求消息请求对终端的认证;

C）认证中心对终端进行认证，同时生成所述终端与所述信令代理的会话密钥，并在注册认证通过后，交由软交换通过信令代理向终端分发所述会话密钥。

10、根据权利要求 9 所述的密钥分发方法，其特征在于，步骤 C）中，认证中心采用下述步骤对终端进行认证:

C1）认证中心根据与终端的共享密钥 Kc 以及与信令代理的共享

密钥 Ksp 生成对终端的第一验证字，然后以所述共享密钥 Kc 和所述共享密钥 Ksp 分别对会话密钥进行加密，将加密后的会话密钥和所述第一验证字返回给软交换；

C2）软交换通过信令代理向终端返回注册失败响应消息通知终端注册失败；

C3）终端根据与认证中心的共享密钥 Kc 生成第二验证字，然后将包含所述第二验证字的注册消息发送给信令代理，由所述信令代理向软交换转发所述注册消息重新进行注册；

C4）软交换根据所述第一验证字和所述第二验证字对所述终端进行认证。

11、根据权利要求 10 所述的密钥分发方法，其特征在于，步骤 C）中，所述软交换采用下述步骤向终端分发所述会话密钥：

C5）软交换向信令代理转发终端注册成功响应消息，所述注册成功响应消息中包含认证中心分别以共享密钥 Kc 和 Ksp 加密后的会话密钥，信令代理用共享密钥 Ksp 解密认证中心经共享密钥 Ksp 加密过的会话密钥，并以所述解密获取的会话密钥对注册成功响应消息报文计算报文验证字，然后信令代理向终端转发注册成功响应消息，所述注册成功响应消息中包含经共享密钥 Kc 加密过的会话密钥以及所述报文验证字；

C6）终端根据所述共享密钥 Kc 解密认证中心加密过的会话密钥，并利用解密后获取的会话密钥，验证信令代理返回报文的报文验证字以验证信令代理身份，同时验证报文的完整性以及信令代理返回的终端自己的安全能力参数是否正确。

12、根据权利要求 11 所述的密钥分发方法，其特征在于，所述方法还包括：终端将包含自身支持的安全能力列表以及每种安全能力的优先级信息的注册消息发送给信令代理，信令代理根据终端支持的安全能力和每种安全能力的优先级信息选择一个合适的安全能力进行通信。

13、根据权利要求 9-12 任一项所述密钥分发方法，其特征在于，

所述注册请求消息和注册消息均为 SIP 协议注册消息，所述注册失败响应消息为 SIP 协议响应消息，所述注册成功响应消息为 SIP 协议注册请求成功消息。

14、根据权利要求 9-12 任一项所述密钥分发方法，其特征在于，所述注册请求消息为 MGCP 协议系统重启消息及其响应消息，所述注册失败响应消息和注册成功响应消息均为 MGCP 协议通知请求消息及其响应消息，所述注册消息为 MGCP 协议通知消息及其响应消息。

15、根据权利要求 9-12 任一项所述密钥分发方法，其特征在于，所述注册请求消息为 H.248 协议系统服务状态变化消息及其响应消息，所述注册失败响应消息和注册成功响应消息均为 H.248 协议属性更改消息及其响应消息，所述注册消息为 H.248 协议通知消息及其响应消息。

16、根据权利要求 9-12 任一项所述密钥分发方法，其特征在于，所述注册请求消息为 H.323 协议网守请求消息，所述注册失败响应消息为 H.323 协议网守拒绝消息，所述注册消息为 H.323 协议注册请求消息，所述注册成功响应消息为 H.323 协议注册成功消息。

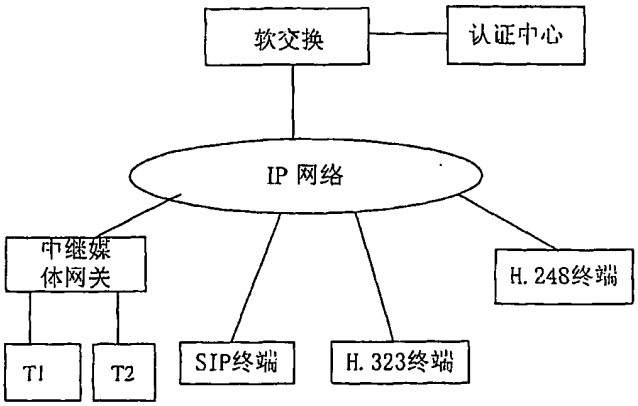

软交换
认证中心
IP 网络
中继媒体网关
H. 248终端
T1
T2
SIP终端
H. 323终端

图 1

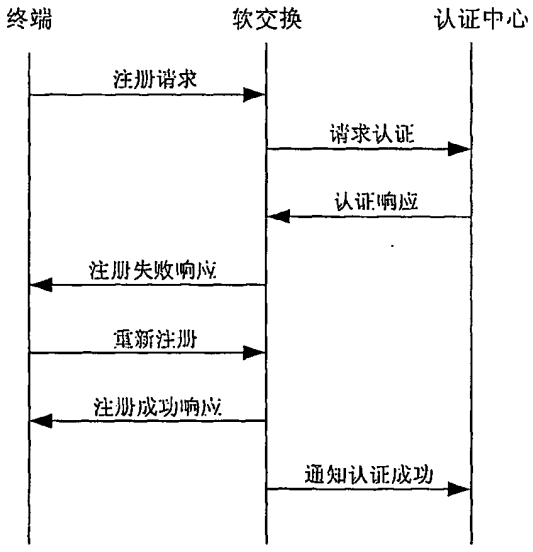

终端
软交换
认证中心
注册请求
请求认证
认证响应
注册失败响应
重新注册
注册成功响应
通知认证成功

图 2

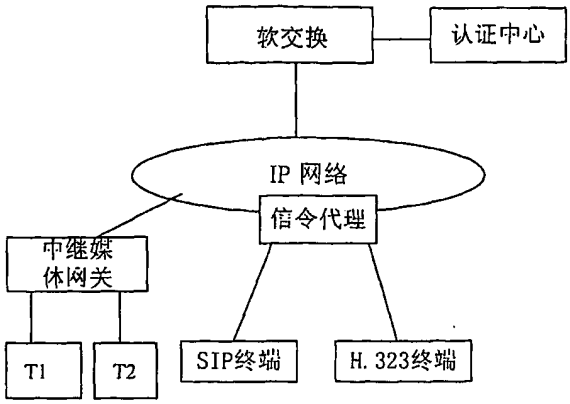


图 3

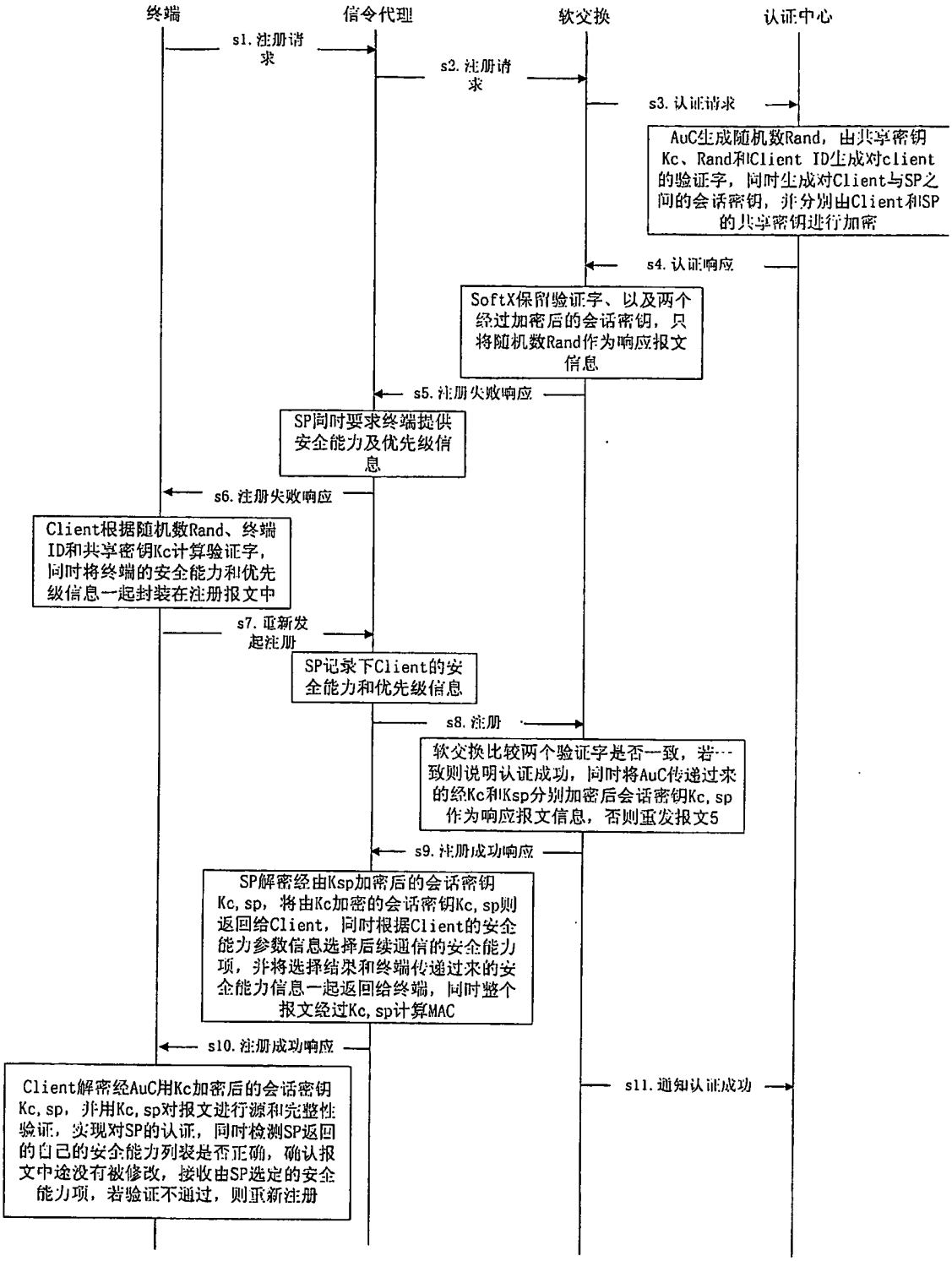

终端
信令代理
软交换
认证中心
s1. 注册请求
s2. 注册请求
s3. 认证请求
AuC生成随机数Rand，由共享密钥Kc、Rand和Client ID生成对client的验证字，同时生成对Client与SP之间的会话密钥，并分别由Client和SP的共享密钥进行加密
s4. 认证响应
SoftX保留验证字、以及两个经过加密后的会话密钥，只将随机数Rand作为响应报文信息
s5. 注册失败响应
SP同时要求终端提供安全能力及优先级信息
s6. 注册失败响应
Client根据随机数Rand、终端ID和共享密钥Kc计算验证字，同时将终端的安全能力和优先级信息一起封装在注册报文中
s7. 重新发起注册
SP记录下Client的安全能力和优先级信息
s8. 注册
软交换比较两个验证字是否一致，若一致则说明认证成功，同时将AuC传递过来的经Kc和Ksp分别加密后会话密钥Kc, sp作为响应报文信息，否则重发报文5
s9. 注册成功响应
SP解密经由Ksp加密后的会话密钥Kc, sp，将由Kc加密的会话密钥Kc, sp则返回给Client，同时根据Client的安全能力参数信息选择后续通信的安全能力项，并将选择结果和终端传递过来的安全能力信息一起返回给终端，同时整个报文经过Kc, sp计算MAC
s10. 注册成功响应
Client解密经AuC用Kc加密后的会话密钥Kc, sp，并用Kc, sp对报文进行源和完整性验证，实现对SP的认证，同时检测SP返回的自己的安全能力列表是否正确，确认报文中途没有被修改，接收由SP选定的安全能力项，若验证不通过，则重新注册
s11. 通知认证成功

图 4

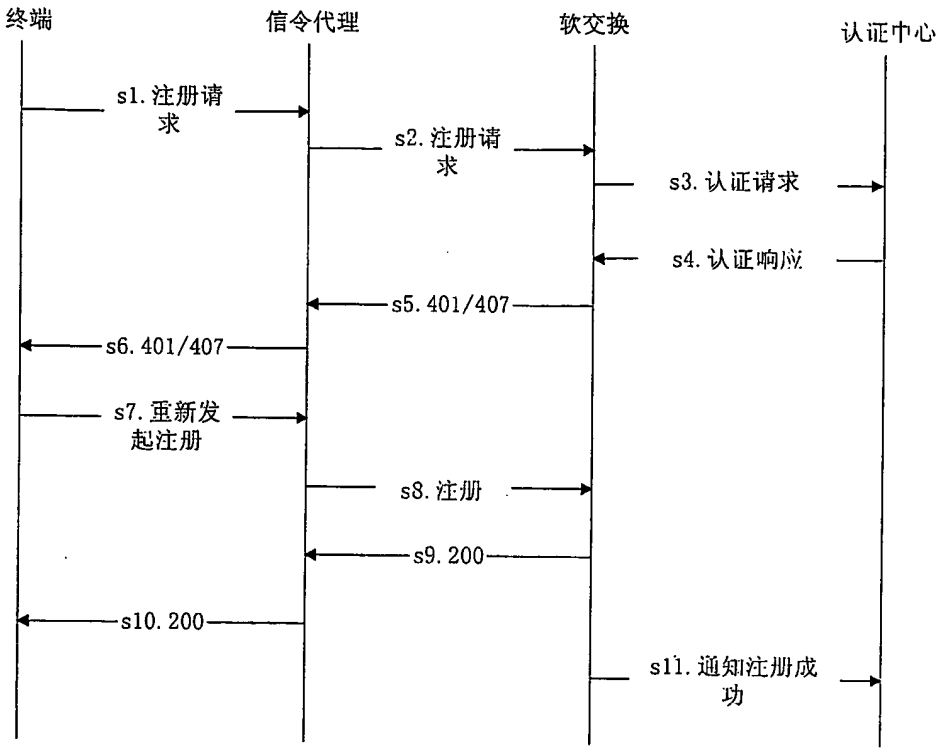

终端
信令代理
软交换
认证中心
s1. 注册请求
s2. 注册请求
s3. 认证请求
s4. 认证响应
s5. 401/407
s6. 401/407
s7. 重新发起注册
s8. 注册
s9. 200
s10. 200
s11. 通知注册成功

图 5

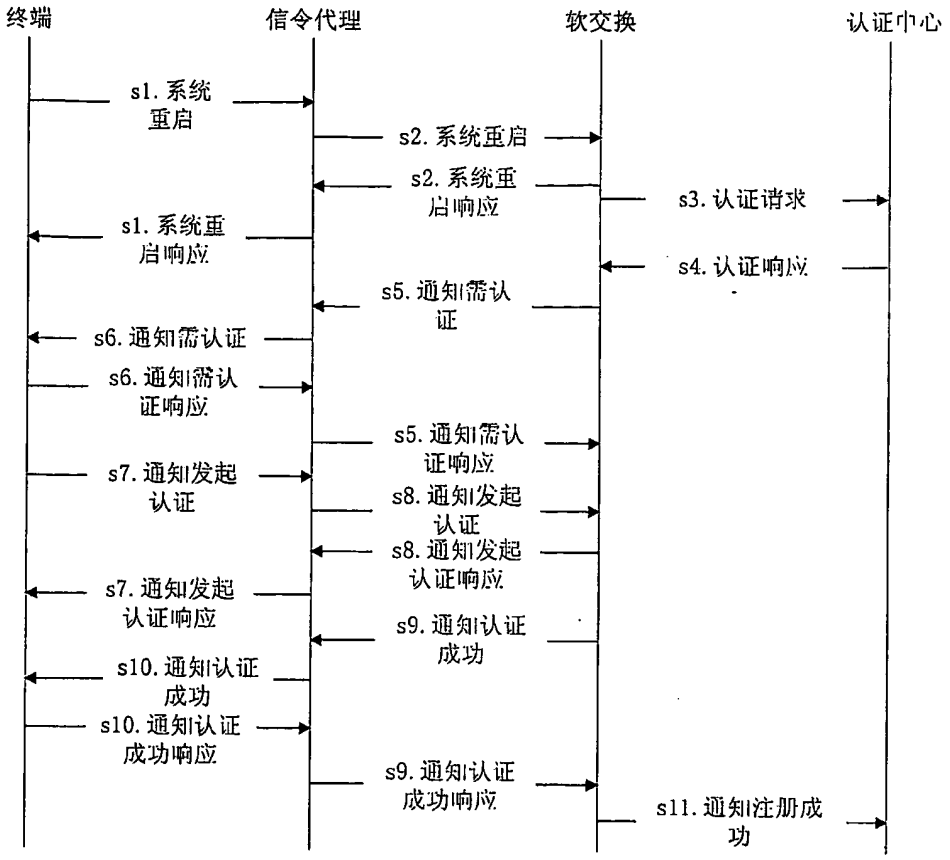

终端
信令代理
软交换
认证中心
s1. 系统重启
s2. 系统重启
s2. 系统重启响应
s3. 认证请求
s1. 系统重启响应
s4. 认证响应
s5. 通知需认证
s6. 通知需认证
s6. 通知需认证响应
s5. 通知需认证响应
s7. 通知发起认证
s8. 通知发起认证
s8. 通知发起认证响应
s7. 通知发起认证响应
s9. 通知认证成功
s10. 通知认证成功
s10. 通知认证成功响应
s9. 通知认证成功响应
s11. 通知注册成功

图 6

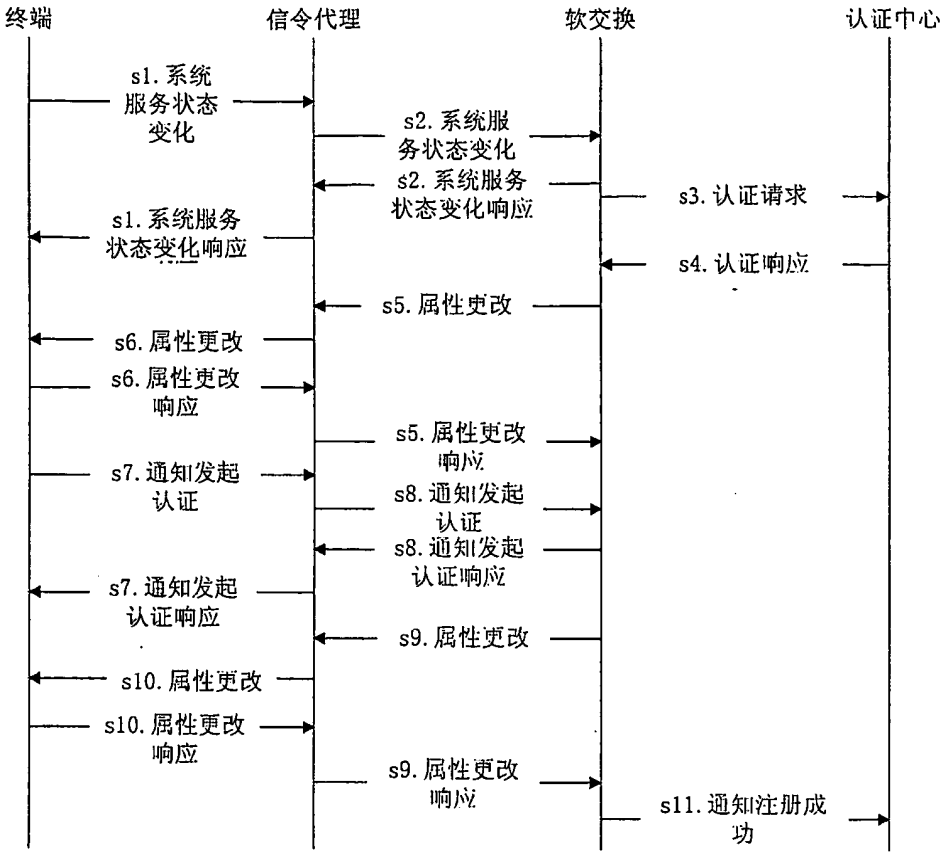

终端
信令代理
软交换
认证中心
s1. 系统服务状态变化
s2. 系统服务状态变化
s2. 系统服务状态变化响应
s3. 认证请求
s1. 系统服务状态变化响应
s4. 认证响应
s5. 属性更改
s6. 属性更改
s6. 属性更改响应
s5. 属性更改响应
s7. 通知发起认证
s8. 通知发起认证
s8. 通知发起认证响应
s7. 通知发起认证响应
s9. 属性更改
s10. 属性更改
s10. 属性更改响应
s9. 属性更改响应
s11. 通知注册成功

图 7

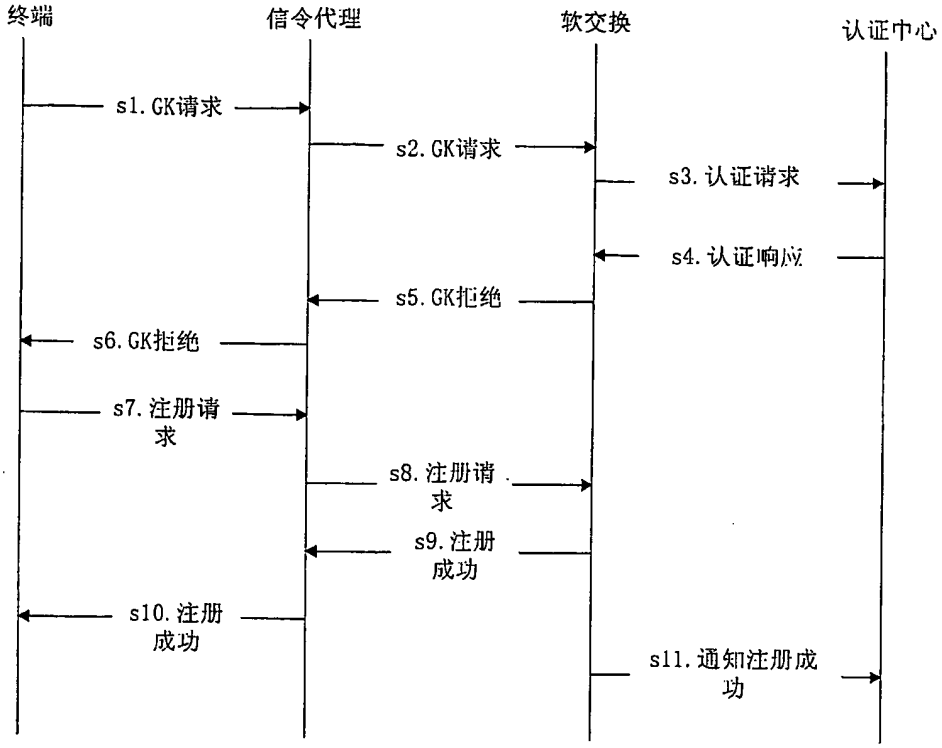

终端
信令代理
软交换
认证中心
s1. GK请求
s2. GK请求
s3. 认证请求
s4. 认证响应
s5. GK拒绝
s6. GK拒绝
s7. 注册请求
s8. 注册请求
s9. 注册成功
s10. 注册成功
s11. 通知注册成功

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2005/000133

A. CLASSIFICATION OF SUBJECT MATTER

IPC[7]:H04L9/32 H04L12/56 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7]:H04L9 H04L12 H04Q7

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, PAJ, CNPAT,CNKI: WPI, EPODOC, PAJ, CNPAT,CNKI: key, certificat+, authenticat+, switch, softswitch+, request, register, login, session

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US2003033521A1 (SAHLBACH A) 13.Feb.2003 (13.02.2003) the whole documnet	1-16
A	US6490358B1 (OPEN MARKET INC) 03.Dec.2002 (03.12.2002) the whole documnet	1-16
A	WO03053074A1 (RUCKSTUHL H) 26.Jun.2003 (26.06.2003) the whole documnet	1-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
01.Sep. 2005 (01.09.2005)	15 · SEP 2005 (15 · 09 · 2005)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer LiuBin Telephone No. (86-10)62084534

Form PCT/ISA /210 (second sheet) (April 2005)

TERNATIONAL SEARCH REPORT

Information patent family members

Search request No.
PCT/CN2005/000133

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US2003033521A1	13.02.2003	NONE	
US6490358B1	03.12.2002	US6212634B1	03.04.2001
WO03053074A1	26.06.2003	DE50202595G	28.04.2005
		AU2002360906A1	30.06.2003
		EP1457062A1	15.09.2004
		DE10295909T	11.11.2004
		EP1457062B1	23.03.2005
		US2005068937A1	31.03.2005

国际检索报告

国际申请号
PCT/CN2005/000133

A. 主题的分类

IPC[7]:H04L9/32 H04L12/56 H04Q7/38

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC[7]:H04L9 H04L12 H04Q7

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI, EPODOC, PAJ, CNPAT,CNKI: key, certificat+, authenticat+, switch, softswitch+, request, register, login, session, 密钥, 认证, 交换, 软交换, 请求, 注册, 会话

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	US2003033521A1 （SAHLBACH A） 13.2 月 2003 (13.02.2003) 全文	1-16
A	US6490358B1 （OPEN MARKET INC） 03.12 月 2002 (03.12.2002) 全文	1-16
A	WO03053074A1 （RUCKSTUHL H） 26.6 月 2003 (26.06.2003) 全文	1-16

☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
01.9 月 2005（01.09.2005）	15 · 9月 2005 (15 · 09 · 2005)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 刘斌 电话号码：(86-10)62084534

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2005/000133

检索报告中引用的专利文件	公布日期	同族专利	公布日期
US2003033521A1	13.2 月 2003	无	
US6490358B1	03.12 月 2002	US6212634B1	03.04.2001
WO03053074A1	26.6 月 2003	DE50202595G	28.04.2005
		AU2002360906A1	30.06.2003
		EP1457062A1	15.09.2004
		DE10295909T	11.11.2004
		EP1457062B1	23.03.2005
		US2005068937A1	31.03.2005